NAŘÍZENÍ KOMISE (ES) č. 482/2008

ze dne 30. května 2008,

kterým se stanoví systém zajištění bezpečnosti softwaru, který má být zaveden poskytovateli letových navigačních služeb, a kterým se mění příloha II nařízení (ES) č. 2096/2005

(Text s významem pro EHP)

KOMISE EVROPSKÝCH SPOLEČENSTVÍ,

s ohledem na Smlouvu o založení Evropského společenství,

s ohledem na nařízení Evropského parlamentu a Rady (ES) č. 550/2004 ze dne 10. března 2004 o poskytování letových navigačních služeb v jednotném evropském nebi (nařízení o poskytování služeb) ([1]), a zejména na článek 4 uvedeného nařízení,

vzhledem k těmto důvodům:

(1) Podle nařízení (ES) č. 550/2004 Komise určí a přijme bezpečnostní předpisy Eurocontrolu (ESARR), přičemž vezme v úvahu stávající právní úpravu Společenství. ESARR 6 nazvaný „Software v systémech ATM" stanoví soubor bezpečnostních předpisů pro zavedení systému zajištění bezpečnosti softwaru.

(2) Nařízení Komise (ES) č. 2096/2005 ze dne 20. prosince 2005, kterým se stanoví společné požadavky pro poskytování letových navigačních služeb ([2]), stanoví v poslední větě dvanáctého bodu odůvodnění, že „Příslušná ustanovení požadavků ESARR 1 pro bezpečnostní dohled při ATM a požadavků ESARR 6 pro software v systémech ATM by měla být určena a přijata formou oddělených právních aktů Společenství."

(3) Příloha II nařízení (ES) č. 2096/2005 požaduje, aby poskytovatelé letových provozních služeb používali systém řízení bezpečnosti a rovněž bezpečnostní požadavky pro posuzování a zmírňování rizika s ohledem na změny. V rámci systému řízení bezpečnosti a jako součást činností týkajících se posuzování a zmírňování rizika s ohledem na změny by poskytovatelé letových provozních služeb měli určit a zavést systém zajištění bezpečnosti softwaru, který by se výslovně zabýval aspekty týkajícími se softwaru.

(4) Hlavním cílem v oblasti bezpečnosti softwaru, který by měly splnit funkční systémy obsahující software, je snížení rizik spojených s používáním softwaru v systémech evropské sítě pro řízení letového provozu („software EATMN") na přijatelnou úroveň.

(5) Toto nařízení by se nemělo vztahovat na vojenské činnosti a výcvik podle čl. 1 odst. 2 nařízení Evropského parlamentu a Rady (ES) č. 549/2004 ze dne 10. března 2004, kterým se stanoví rámec pro vytvoření jednotného evropského nebe (rámcové nařízení) ([3]).

(6) Příloha II nařízení (ES) č. 2096/2005 by tudíž měla být změněna.

(7) Opatření stanovená tímto nařízením jsou v souladu se stanoviskem Výboru pro jednotné nebe,

PŘIJALA TOTO NAŘÍZENÍ:

Článek 1

Předmět a oblast působnosti

1. Toto nařízení stanoví požadavky na určení a zavedení systému zajištění bezpečnosti softwaru poskytovateli letových provozních služeb (ATS), subjekty zajišťujícími uspořádání toku letového provozu (ATFM) a uspořádání vzdušného prostoru (ASM) pro všeobecný letový provoz a poskytovateli komunikačních, navigačních a pozorovacích služeb (CNS).

Nařízení určuje a schvaluje povinná ustanovení bezpečnostních regulačních požadavků organizace Eurocontrol – ESARR 6, nazvaná „Software v systémech ATM", vydaných dne 6. listopadu 2003.

2. Toto nařízení se použije na nový software a veškeré změny softwaru v systémech ATS, ASM, ATFM a CNS.

Nepoužije se na software palubních prvků ani na zařízení v kosmickém prostoru.

Článek 2

Definice

Pro účely tohoto nařízení se použijí definice uvedené v článku 2 nařízení (ES) č. 549/2004.

([1]) Úř. věst. L 96, 31.3.2004, s. 10.

([2]) Úř. věst. L 335, 21.12.2005, s. 13. Nařízení ve znění nařízení (ES) č. 1315/2007 (Úř. věst. L 291, 9.11.2007, s. 16).

([3]) Úř. věst. L 96, 31.3.2004, s. 1.

Rovněž se použijí tyto definice:

1) „softwarem“ se rozumí počítačové programy a odpovídající konfigurační data, včetně nevyvíjeného softwaru, s výjimkou elektronických prvků, jako jsou aplikace určitých integrovaných obvodů, programovatelných logických obvodů nebo logické přepínače v ustáleném stavu;

2) „konfiguračními daty“ se rozumí data, která konfigurují druhový softwarový systém v jednotlivých případech použití;

3) „nevyvíjeným softwarem“ se rozumí software, který nebyl vyvinut pro stávající smlouvu;

4) „zajištěním bezpečnosti“ se rozumí veškeré plánované a systematické činnosti nezbytné k poskytování přiměřené jistoty, že výrobek, služba, organizace nebo funkční systém dosahuje přijatelné nebo přípustné bezpečnosti;

5) „organizací“ se rozumí poskytovatel ATS, poskytovatel CNS nebo subjekt zajišťující ATFM nebo ASM;

6) „funkčním systémem“ se rozumí kombinace systémů, postupů a lidských zdrojů, které jsou uspořádány tak, aby plnily určitou funkci v rámci ATM;

7) „rizikem“ se rozumí kombinace celkové pravděpodobnosti nebo četnosti výskytu škodlivého účinku vyvolaného nebezpečím a závažnosti tohoto účinku;

8) „nebezpečím“ se rozumí jakýkoliv stav, událost nebo okolnost, která by mohla vyvolat nehodu;

9) „novým softwarem“ se rozumí software, který byl objednán nebo na který byly podepsány závazné smlouvy po vstupu tohoto nařízení v platnost;

10) „bezpečnostním cílem“ se rozumí kvalitativní nebo kvantitativní výrok, který určuje nejvyšší četnost nebo pravděpodobnost, s níž se podle očekávání může vyskytnout nebezpečí;

11) „bezpečnostním požadavkem“ se rozumí prostředek pro zmírnění rizika, určený strategií zmírňování rizik, který splňuje určitý bezpečnostní cíl a zahrnuje organizační, provozní, procedurální, funkční a výkonnostní požadavky, požadavky interoperability nebo charakteristiku prostředí;

12) „přepnutím nebo výměnou za provozu“ se rozumí způsob výměny prvků systému evropské sítě pro řízení letového provozu (EATMN) nebo softwaru za provozu systému;

13) „bezpečnostním požadavkem na software“ se rozumí popis toho, co má software vytvářet při daných vstupech a omezeních a co v případě splnění zajistí, že software EATMN pracuje bezpečně a v souladu s provozními potřebami;

14) „softwarem EATMN“ se rozumí software používaný v EATM podle článku 1;

15) „platností požadavků“ se rozumí potvrzení na základě zkoumání a poskytnutí objektivního důkazu, že jsou splněny konkrétní požadavky zamýšleného použití;

16) „nezávislým dosažením“ se v případě činností v rámci procesu ověřování softwaru rozumí, že činnosti v rámci procesu ověřování provádí jiná osoba (jiné osoby) než osoba, která ověřovaný prvek vyvinula;

17) „poruchou softwaru“ se rozumí neschopnost programu správně vykonávat požadovanou funkci;

18) „selháním softwaru“ se rozumí neschopnost programu vykonávat požadovanou funkci;

19) „aplikací COTS“ (*Commercial Off-The-Shelf*) se rozumí komerčně dostupná aplikace, kterou prodávají obchodníci prostřednictvím veřejně dostupných katalogů a která není určena pro úpravu podle požadavků zákazníka nebo zdokonalování;

20) „složkami softwaru“ se rozumí moduly, které lze instalovat nebo kombinovat s jinými opakovaně využitelnými softwarovými moduly k vytvoření softwarové aplikace podle požadavků zákazníka;

21) „nezávislými prvky softwaru“ se rozumí prvky softwaru, které nevyřadí z provozu stejné selhání, jímž je způsobeno nebezpečí;

22) „reakční dobou softwaru“ se rozumí čas, během něhož má software reagovat na dané vstupy nebo periodické události a/nebo výkon softwaru z hlediska transakcí nebo zpráv zpracovaných za jednotku času;

23) „kapacitou softwaru“ se rozumí schopnost softwaru zpracovat daný objem toku dat;

24) „přesností“ se rozumí požadovaná přesnost vypočtených výsledků;

25) „využitím zdrojů“ se rozumí objem zdrojů výpočetního systému, které může aplikační software využívat;

26) „odolností softwaru“ se rozumí chování softwaru v případě neočekávaných vstupů, poruch hardwaru a přerušení dodávky elektřiny buď přímo do výpočetního systému, nebo do připojených zařízení;

27) „tolerancí přetížení“ se rozumí chování systému, a zejména jeho tolerance v případě výskytu většího objemu vstupů, než je objem očekávaný při běžném provozu systému;

28) „správným a úplným ověřením softwaru EATMN“ se rozumí všechny požadavky na bezpečnost softwaru, které správně stanoví, co vyžaduje postup pro posuzování a zmírňování rizika od prvků softwaru, a jejich zavedení prokazatelně dosahuje požadované úrovně bezpečnosti softwaru;

29) „daty životního cyklu softwaru“ se rozumí data vytvořená během životního cyklu softwaru, která slouží plánování, řízení, vysvětlování, určování, zaznamenávání nebo poskytování důkazů o činnostech; tato data umožňují schvalování procesů životního cyklu softwaru, systémů nebo zařízení a modifikaci softwarového produktu po schválení;

30) „životním cyklem“ se rozumí:

a) objednaný soubor postupů určených organizací jako dostačující a přiměřené pro vytvoření softwarového produktu;

b) časový úsek, který začíná rozhodnutím vytvořit nebo upravit softwarový produkt a končí vyřazením produktu z provozu;

31) „požadavkem na bezpečnost systému“ se rozumí bezpečnostní požadavek odvozený pro funkční systém.

Článek 3

Všeobecné bezpečnostní požadavky

1. Kdykoli má organizace zavést postup pro posuzování a zmírňování rizika v souladu s platnými právními předpisy Společenství nebo vnitrostátními právními předpisy, určí a zavede systém zajištění bezpečnosti softwaru, který se bude zabývat konkrétními aspekty týkajícími se softwaru EATMN, včetně všech provozních změn softwaru on-line, jako je přepnutí nebo výměna za provozu.

2. Organizace zajistí, aby její systém zajištění bezpečnosti softwaru poskytoval alespoň důkazy a argumenty, které svědčí o tom, že:

a) požadavky na bezpečnost softwaru správně stanoví, co se požaduje od softwaru ke splnění bezpečnostních cílů a požadavků stanovených v rámci postupu pro posuzování a zmírňování rizika;

b) je zajištěna sledovatelnost všech požadavků na bezpečnost softwaru;

c) zavedení softwaru neobsahuje žádné funkce, které mají nepříznivý vliv na bezpečnost;

d) software EATMN splňuje na něj kladené požadavky na úrovni jistoty, která je v souladu s kritičností softwaru;

e) je zajištěno splnění všeobecných bezpečnostních požadavků stanovených v písmenech a) až d) a argumenty, jimiž lze toto zajištění prokázat, lze kdykoli odvodit:

i) ze známé spustitelné verze softwaru,

ii) ze známého rozsahu konfiguračních dat,

iii) ze známého souboru softwarových produktů a popisů, včetně specifikací, které byly použity při vytvoření dané verze.

3. Organizace poskytne vnitrostátnímu dozorovému orgánu potřebné záruky, prokazující, že požadavky stanovené v odstavci 2 byly splněny.

Článek 4

Požadavky na systém zajištění bezpečnosti softwaru

Organizace zajistí, aby systém zajištění bezpečnosti softwaru splňoval alespoň tato kritéria:

1) systém je zdokumentovaný výslovně jako součást všeobecné dokumentace posuzování a zmírňování rizika;

2) každému provozovanému softwaru EATMN přiřadí systém úroveň zajištění softwaru v souladu s požadavky stanovenými v příloze I;

3) systém zahrnuje zajištění týkající se:

a) platnosti požadavků na bezpečnost softwaru v souladu s požadavky stanovenými v příloze II části A;

b) ověření softwaru v souladu s požadavky stanovenými v příloze II části B;

c) řízení konfigurace softwaru v souladu s požadavky stanovenými v příloze II části C;

d) sledovatelnosti požadavků na bezpečnost softwaru v souladu s požadavky stanovenými v příloze II části D;

4) systém určuje nároky na úroveň zajištění; nároky musí být stanoveny pro každou úroveň zajištění softwaru a zvyšovány s rostoucí kritičností softwaru; za tím účelem:

a) rozdílné nároky odpovídající jednotlivým úrovním zajištění softwaru musí zahrnovat kritéria:

i) která se musí splnit nezávisle,

ii) která se musí splnit,

iii) která se nemusí splnit;

b) zajištění odpovídající každé úrovni zajištění softwaru musí poskytovat dostatečnou jistotu, že software EATMN lze provozovat s přípustnou mírou bezpečnosti;

5) systém využívá zkušenosti se softwarem EATMN jako zpětnou vazbu pro potvrzení, že systém zajištění bezpečnosti softwaru a přiřazení jednotlivých úrovní zajištění jsou přiměřené. Za tímto účelem se musí účinky poruchy nebo selhání softwaru, vykázané podle příslušných požadavků na vykazování a posuzování bezpečnostních incidentů, posuzovat ve srovnání s účinky stanovenými pro příslušný systém podle schématu klasifikace závažnosti stanoveného v oddílu 3.2.4 přílohy II nařízení (ES) č. 2096/2005.

Článek 5

Požadavky na změny softwaru a na určitý software

1. V případě jakýchkoli změn softwaru nebo určitých druhů softwaru, např. COTS, nevývojového softwaru nebo dříve používaného softwaru, na nějž nelze použít některé z požadavků čl. 3 odst. 2 písm. d) nebo e) nebo čl. 4 odst. 2, 3, 4 nebo 5, organizace zajistí, aby systém zajištění bezpečnosti softwaru poskytoval pomocí jiných prostředků vybraných a odsouhlasených vnitrostátním dozorovým orgánem stejnou úroveň jistoty jako příslušná úroveň zajištění softwaru v případě, že je definovaná.

Tyto prostředky musí poskytovat dostatečnou jistotu, že software splňuje bezpečnostní cíle a požadavky stanovené v rámci postupu pro posuzování a zmírňování rizika.

2. Pro posouzení prostředků uvedených v odstavci 1 může vnitrostátní dozorový orgán použít uznávanou organizaci nebo oznámený subjekt.

Článek 6

Změna nařízení (ES) č. 2096/2005

V příloze II nařízení (ES) č. 2096/2005 se doplňuje nový text, který zní:

„3.2.5 Oddíl 5

Systém zajištění bezpečnosti softwaru

V rámci systému řízení bezpečnosti zavede poskytovatel letových provozních služeb systém zajištění bezpečnosti softwaru v souladu s nařízením Komise (ES) č. 482/2008 (ze dne 30. května 2008, kterým se stanoví systém zajištění bezpečnosti softwaru, který má být zaveden poskytovateli letových navigačních služeb, a kterým se mění nařízení (ES) č. 2096/2005 (*).

(*) Úř. věst. L 141, 31.5.2008, s. 5.“

Článek 7

Vstup v platnost

Toto nařízení vstupuje v platnost dvacátým dnem po vyhlášení v *Úředním věstníku Evropské unie*.

Použije se ode dne 1. ledna 2009 na nový software systémů EATMN uvedený v čl. 1 odst. 2.

Použije se ode dne 1. července 2010 na jakékoli změny softwaru systémů EATMN uvedených v čl. 1 odst. 2, které budou k uvedenému dni v provozu.

Toto nařízení je závazné v celém rozsahu a přímo použitelné ve všech členských státech.

V Bruselu dne 30. května 2008.

Za Komisi

Antonio TAJANI

člen Komise

PŘÍLOHA I

Požadavky na úroveň zajištění softwaru podle čl. 4 odst. 2

1. Úroveň zajištění softwaru musí odpovídat nárokům na zajištění softwaru podle kritičnosti softwaru EATMN v souladu se schématem pro klasifikaci závažnosti stanoveným v příloze II oddílu 4 bodu 3.2.4 nařízení (ES) č. 2096/2005, v kombinaci s pravděpodobností výskytu určitého nepříznivého účinku. Určí se alespoň čtyři úrovně zajištění softwaru, přičemž úroveň zajištění softwaru 1 označuje nejkritičtější úroveň.

2. Přiřazená úroveň zajištění softwaru musí být podle přílohy II oddílu 4 bodu 3.2.4 nařízení (ES) č. 2096/2005 přiměřená nejnepříznivějšímu účinku, jaký mohou poruchy nebo selhání softwaru způsobit. Zohlední se zejména rizika spojená s poruchami nebo selháními softwaru a příslušné ochranné mechanismy na úrovni architektury a/nebo postupů.

3. Prvkům softwaru EATMN, jejichž vzájemnou nezávislost nelze prokázat, se přiřadí úroveň zajištění softwaru odpovídající nejkritičtějším závislým prvkům.

PŘÍLOHA II

Část A: Požadavky na zajištění platnosti požadavků na bezpečnost softwaru podle čl. 4 odst. 3 písm. a)

1. Požadavky na bezpečnost softwaru podle potřeby upřesní funkční chování softwaru EATMN v normálním a zhoršeném režimu, reakční doby, kapacitu, přesnost, využití zdrojů cílového hardwaru, odolnost vůči neobvyklým provozním podmínkám a toleranci přetížení.

2. Požadavky na bezpečnost softwaru musí být úplné a správné a musí být v souladu s požadavky na bezpečnost systému.

Část B: Požadavky na zajištění ověření softwaru uvedené v čl. 4 odst. 3 písm. b)

1. Funkční chování softwaru EATMN, reakční doby, kapacita, přesnost, využití zdrojů cílového hardwaru, odolnost vůči neobvyklým provozním podmínkám a tolerance přetížení musí být v souladu s požadavky na software.

2. Software EATMN musí být přiměřeně ověřen na základě analýzy a/nebo testování a/nebo obdobných prostředků odsouhlasených vnitrostátním dozorovým orgánem.

3. Ověření softwaru EATMN musí být správné a úplné.

Část C: Požadavky na zajištění řízení konfigurace softwaru uvedené v čl. 4 odst. 3 písm. c)

1. Musí existovat takový systém identifikace, sledovatelnosti a evidence konfigurace, který umožní prokázat, že údaje o životním cyklu softwaru podléhají řízení konfigurace po celou dobu trvání životního cyklu softwaru EATMN.

2. Musí existovat takový systém hlášení problémů, sledování a nápravných opatření, který umožní prokázat, že bezpečnostní problémy spojené se softwarem byly zmírněny.

3. Musí existovat takové postupy pro vyhledávání a vydávání dat, které umožní obnovovat a získávat data týkající se životního cyklu softwaru po dobu celého životního cyklu softwaru EATMN.

Část D: Požadavky na zajištění sledovatelnosti požadavků na bezpečnost softwaru podle čl. 4 odst. 3 písm. d)

1. Každý požadavek na bezpečnost softwaru musí být možno sledovat až na úroveň návrhu, kde lze prokázat jeho splnění.

2. Každý požadavek na bezpečnost softwaru na každé úrovni návrhu, na které se prokáže jeho splnění, musí být možno sledovat ve vztahu k požadavkům na bezpečnost systému.